Digital cash and privacy: What are the alternatives to Libra?

MIT Media Lab Follow
Jul 19 • 6 min read

By Christian Grothoff and Alex Pentland

Credit: Facebook

Libra, the new global payment system which Facebook, Mastercard, Visa, PayPal, and other major players plan to launch in 2020, is dominating the news these days, with politicians and regulators scrambling to find an answer to the new payment platform seemingly patterned after the dystopian E-corp of the Mr. Robot series. However, national regulation may not be sufficient in the face of market demand: consumers yearn after a more usable online payment system, and merchants are hoping for a more cost-effective replacement of the current credit-card centered systems. Here, the GNU

project [1] enters the stage with Taler, offering a socially more acceptable, and yet equally transformative payment technology.

What is Libra?

While Facebook calls Libra a “crypto-currency,” its design has little in common with Bitcoin and other decentralized peer-to-peer payment systems. A Libra basically represents a share in a reserve fund which is a basket of established currencies and is therefore a so-called “stable coin.” The exact composition of the basket will be determined and possibly changed by the Libra consortium which is located in Geneva and might thus be regulated by Swiss financial authorities. Swiss regulators are renowned for taking a lightweight approach on crypto-currency regulation. Transactions between Libra wallets will be stored in a ledger using a private blockchain, a database operated by the Libra consortium, with transactions digitally signed by the users making payments. Users will be able to trade Libra for established currencies via the Libra consortium. Facebook expects to cover the costs to operate the system from the interest on the reserve fund, which may be difficult given Europe’s currently non-positive interest rates — unless a big portion is held in US dollars.

KYC/AML vs. privacy

Libra has to properly identify its users to satisfy know-your-customer (KYC) and anti-money-laundering (AML) regulations. Thus, the possibility to create multiple accounts will be meaningless from a privacy perspective, as both the Libra operators and the authorities will be able to track Libra’s users. While this data would be beneficial for the targeted advertising business run by Facebook and to law enforcement, it also enables population control on an unprecedented scale: Libra can tell where users are, see their transactions and also block transactions at a whim. This will create a veritable challenge for regulators to make sure such power is not abused by exhibiting anti-competitive behavior. Libra holdings of foreign citizens may be at risk if the US government imposes broad sanctions.

Centralized vs. decentralized

A fundamental problem with Libra is that it provides an effectively centralized register under the control of the Libra consortium which states who owns how much. This is in stark contrast to decentralized payment systems like coins, cash or Bitcoin where its valuables are held by individuals. As a result, seizing those valuables is more difficult, limiting government's stronghold on individuals. However, such disintermediated decentralized payment systems are problematic as the authorities lack a way to track and block transactions related to illegitimate business.

What is the alternative?

In 1990, the Dutch company DigiCash pioneered a third approach that does not suffer from these drawbacks using so-called untraceable electronic cash. DigiCash provided asymmetric anonymity: offering privacy for buyers while ensuring transparency for sellers. While DigiCash went bankrupt, a modern implementation of their approach is provided by Taler Systems SA as Free Software with the "GNU Taler" protocol [2]. In Taler, a payment service provider issues untraceable electronic coins to consumers, which holds these valuable tokens in electronic wallets on their own devices. They can then spend those coins like cash at merchants without disclosing their identity — unless legally required to do. For the transaction to be assured, merchants have to deposit the coins with the payment service provider, thereby revealing their income to the state. This income transparency makes the system unattractive for criminal activity, while the funds held in citizen's wallets preserve their personal liberty. In addition, the Taler system is so efficient that it enables micropayments which has the potential to become disruptive in many ways.

Monetary policy. national money vs. transnational money

Libra and Taler also differ with respect to their impact on national sovereignty: Libra is intended to work with a basket of currencies, thereby creating de facto a new currency which is possibly impacting the monetary

policies of the underlying currencies if it becomes big enough. While consumers may relish the simplicity of using one currency for transactions on a global scale, the Eurozone continues to demonstrate the difficult challenges which arise when imposing a transnational monetary policy on diverging national economies. With the Libra consortium a private entity will determine the composition of the assets backing the Libra, and thus may gain significant political power.

In contrast, Taler can be deployed with many different currencies and allows different policies to be used for its asset backing. For example, Taler could be denominated in one national currency and subjected to the respective nation's laws and regulations. Such a deployment could be offered by commercial banks that satisfy the associated regulatory requirements, or be instantiated by the respective central bank and issued as a central bank digital currency (CBDC), i.e. as a liability of the central bank. In this case, Taler would be the digital equivalent of a banknote.

Eliminating selfish policies with TradeCoin

For transnational payments, an international Taler denomination could be created which would, for example, be backed by real-world assets. As with Libra, a simplistic design creates the issue of the entity determining the asset-backing to allocate assets in a self-serving manner. A possible solution to this is TradeCoin, a permissioned blockchain currently under development at MIT [3]. With TradeCoin, alliances of say broadly-based stewards of individuals wealth such as retirement funds or sovereign wealth funds could band together to establish their own denomination and pool their resources and reputations to compete with established national currencies. TradeCoin would then be used to record larger transactions in the ledger provided by the provisioned blockchain, while the combination with Taler provides consumers with private microtransactions.

An open challenge for both Libra and TradeCoin is a way to globally support Know-Your-Customer (KYC) and Anti-Money-Laundering (AML) regulation without relying on an existing banking system. This is particularly difficult

given that today KYC and AML policies arise from the politics of a few large countries.

The Libra consortium and developing countries

Libra's unprecedented consortium of mega-corporations is also threatening the emerging banking systems of developing countries. For consumers, moving savings into a Libra wallet may provide a safe heaven from banks with their high fees and traditional processes. However, we should not expect Visa, MasterCard and PayPal to simply give up their highly lucrative businesses, especially once they have stopped competing with each other by forming a joint business in the Libra consortium. Taler also aims to become a global standard, but with multiple banks being able to deploy their own payment service processor using Free Software — Taler would foster rather than endanger a competitive payment service marketplace. Finally, a combination with TradeCoin would empower groups of smaller nations to pursue sovereign monetary policies benefiting their own economies.

Conclusion

The next years will show the results of this battle of 3rd generation cryptographic payment systems. While Facebook has the user-base, it is dragged by its record on privacy. Also, the Libra design can expect to face an uphill battle from monetary policy to anti-trust regulation. With the Taler system, banks could yet find a way to compete in online payments exploiting their existing core assets, such as the consumer's trust in banking secrecy and national regulations.

[1] https://www.gnu.org/

[2] https://taler.net/

[3] https://tradecoin.mit.edu/

. . .

This post was originally published on the Media Lab website.